Remarks

1. Summary of Office Action

In the Office Action mailed on August 9, 2004, the Examiner rejected claims 1, 2, 5, 8, 9, 13, 14, 17, 20, 21, 25, 26, 30-32, and 36 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,105,134 (Pinder et al., hereinafter "Pinder"). Further, the Examiner rejected claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 34 under 35 U.S.C. § 103(a) as being obvious over a combination of Pinder and U.S. Patent No. 4,731,840 (Mniszewski et al., hereinafter "Mniszewski"), and claims 10 and 22 as being obvious over a combination of Pinder and U.S. Patent No. 5,124,117 (Tatebayashi et al., hereinafter "Tatebayashi").

2. Amendments

Applicants have amended claims 1, 2, 13, 14, 25, 31, and 33 to recite the invention more particularly, as fully supported by Applicants' specification. Applicants have also canceled claims 5, 6, 7, 17, 18, and 19 and added new claims 37-42, including two independent claims 37 and 40, for which additional fee is enclosed herein.

Pending in this application are claims 1-4, 8-16, and 20-42, of which claims 1, 13, 25, 31, 37, and 40 are independent and the remainder are dependent.

3. Response to § 102 Rejections

As noted above, the Examiner rejected claims 1, 2, 5, 8, 9, 13, 14, 17, 20, 21, 25, 26, 30-32, and 36 under 35 U.S.C. § 102(e) as being anticipated by Pinder.

Under M.P.E.P. § 2131, a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. Applicants have canceled claims 5 and 17 without prejudice, and thus respectfully traverse the Examiner's rejections as moot with respect to these claims. Applicants respectfully traverse the

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

rejections of claims 1, 2, 8, 9, 13, 14, 20, 21, 25, 26, 30-32, and 36 because Pinder does not disclose or suggest each and every element of any one of these claims. Applicants also traverse this rejection with respect to new claims 37-42 presently pending in the application, because Pinder fails to disclose or suggest every element of any of these claims.

Applicants' claims are directed to providing secure communications between network devices. In particular, each of independent claims 1, 13, and 25, as amended above, recites in various ways the limitations of (i) using a first encryption key to encrypt and decrypt communications between a first and a second network device, *the first encryption key including both a (first) base key and a key extension in addition to the (first) base key*, and (ii) using a second encryption key (that includes a (second) base key) to encrypt and decrypt communications between the second and a third network device, *wherein security determined by the first encryption key is stronger than security determined by the second encryption key.*

Similarly, each of independent claims 31, 37, and 40, as amended above, recites, in one way or another, the limitations of (i) using a first authorization key to negotiate a first encryption key for encrypting and decrypting communications between a first and a second network device, *the first authorization key including both a (first) base key and a key extension in addition to the (first) base key*, and (ii) using a second authorization key (that includes a (second) base key) to negotiate a second encryption key for encrypting and decrypting communications between the second and a third network device, *wherein security determined by the first encryption key is stronger than security determined by the second encryption key.*

Generally, Pinder teaches a system that uses symmetrical key encryption techniques to encrypt and decrypt service instances (e.g., programs) provided by a service origination component (e.g., a service distribution organization, such as a cable headend) to a service

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

reception component (e.g., a set-top box). In particular, as taught by Pinder, the service origination component uses an encryption key called a "control word" to encrypt a given service instance and distributes the encrypted service instance to service reception components. In turn, service reception components, such as set-top boxes, authorized to receive the given service instance, use the control word to decrypt the encrypted service instance for viewing by a subscriber. (*See* Pinder, e.g., Figure 3 and the accompanying text.)

To ensure that only an authorized set-top box is capable of decrypting the encoded service instance, Pinder's system relies on information provided in entitlement control messages (ECMs) and entitlement management messages (EMMs). Specifically, as disclosed by Pinder, security is provided by the fact that service instance identification information included in the ECM must agree with the authorization information received in the EMM before the control word is provided to a service decryptor of a set-top box to decrypt the service instance. (*See* Pinder, e.g., col. 9, line 67 to col. 10, lines 1-4.)

Applicants, however, do not find in Pinder the combination of elements recited in any of independent claims 1, 13, 25, 31, 37, and 40.

In particular, Applicants do not find in Pinder any disclosure of the presently claimed limitations of (i) using a first encryption key to encrypt and decrypt communications between a first and a second network device, *the first encryption key including both a (first) base key and a key extension in addition to the (first) base key*, and (ii) using a second encryption key (that includes a (second) base key) to encrypt and decrypt communications between the second and a third network device, *wherein security determined by the first encryption key is stronger than security determined by the second encryption key.*

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Similarly, Applicants do not find in Pinder any disclosure of (i) using a first authorization key to negotiate a first encryption key for encrypting and decrypting communications between a first and a second network device, *the first authorization key including both a (first) base key and a key extension in addition to the (first) base key*, and (ii) using a second authorization key (that includes a (second) base key) to negotiate a second encryption key for encrypting and decrypting communications between the second and a third network device, *wherein security determined by the first encryption key is stronger than security determined by the second encryption key.*

Rather, a person skilled in the art would logically understand that Pinder merely teaches a system in which information included in EMMs and ECMs is used in combination to determine whether a particular set-top box is authorized to decrypt a given service instance. In fact, at col. 9, lines 50-55, Pinder makes clear that

> "The identifying information [from the ECM] is used together with the authorization information received with EMM 315 to determine whether DHCT 333 [i.e., a set-top box] is authorized to receive the service instance 325. If it is, control word 319 is used in the service decryptor 347 to decrypt encrypted content to produce original content 325."

Pinder, however, does not teach a system in which a degree of security used for communications between a first network device and a second network device, and between the second network device and a third network device can be selectively varied by including a key extension in an encryption key or an authorization key, as claimed by Applicants.

Advantageously, with Applicants claimed invention, the use of a first encryption key with a longer bit length (e.g., by including a key extension in the first encryption key) allows the first and second network devices to communicate using stronger security, while the use of a second encryption key with a shorter bit length (e.g., by excluding a key extension in the second

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

encryption key) prevents the second and third network devices from implementing stronger security.

Because Pinder fails to teach all of the limitations of any of claims 1, 13, 25, 31, 37, and 40, Pinder fails to anticipate these claims under 35 U.S.C. § 102. Claims 2, 8, 9, 14, 20, 21, 26, 30, 32, 36, 38, 39, 41, and 42 depend from respective claim 1, 13, 25, 31, 37, and 40 and therefore incorporate all of the elements of claim 1, 13, 25, 31, 37, or 40. Therefore, Pinder also fails to anticipate claims 2, 8, 9, 14, 20, 21, 26, 30, 32, 36, 38, 39, 41, and 42.

4. Response to § 103 Rejections

As noted further above, the Examiner rejected claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 34 under 35 U.S.C. § 103(a) as being obvious over a combination of Pinder and Mniszewski, and claims 10 and 22 as being obvious over a combination of Pinder and Tatebayashi.

a. Claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 34

The Examiner rejected claims 3, 4, 6, 7, 15, 16, 18, 19, 27, 28, 33, and 34 on grounds of obviousness over the combination of Pinder and Mniszewski.

In order to establish a *prima facie* case of obviousness of a claimed invention by applying a combination of references, the prior art must teach or suggest all of the claim limitations. M.P.E.P. § 2143. Applicants have canceled claims 6, 7, 18, and 19 without prejudice, and thus respectfully traverse the Examiner's rejections as moot with respect to these claims. Applicants also respectfully traverse the rejections of claims 3, 4, 15, 16, 27, 28, 33, and 34, because the combination of Pinder and Mniszewski fails to disclose or suggest every element of any of claims 3, 4, 15, 16, 27, 28, 33, and 34.

Each of claims 3, 4, 15, 16, 27, 28, 33, and 34 depends from respective claim 1, 11, 25, or 31 and therefore incorporates the limitations of claim 1, 13, 25, or 31. As discussed above,

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Pinder fails to teach the invention of any of claims 1, 13, 25, and 31. Therefore, Pinder also fails to teach or suggest the invention as recited in any of claims 3, 4, 15, 16, 27, 28, 33, and 34. Further, Applicants respectfully submit that Mniszewski fails to overcome the deficiencies of Pinder described above.

Applicants do not concede that the representations made more specifically by the Examiner with respect to dependent claims 3, 4, 15, 16, 27, 28, 33, and 24 are correct. However, Applicants submit that those other points are moot in view of the fact that the cited combination fails to teach or suggest the invention as recited in any of independent claims 1, 13, 25, and 31.

b. Claims 10 and 22

Next, the Examiner rejected claims 10 and 22 on grounds of obviousness over the combination of Pinder and Tatebayashi.

As noted above, in order to establish a *prima facie* case of obviousness of a claimed invention by applying a combination of references, the proposed combination must teach or suggest all of the elements of the claimed invention. Applicants respectfully traverse the rejections of claims 10 and 22, because the combination of Pinder and Tatebayashi fails to disclose or suggest the invention as recited in any of these claims.

Claim 10 ultimately depends from claim 1 and therefore incorporates all of the elements of claim 1. Claim 22 ultimately depends from claim 13 and therefore incorporates all of the elements of claim 13. As discussed above, Pinder fails to teach or suggest the invention as recited in each of claims 1 and 13. Therefore, Pinder fails to teach or suggest the invention as recited in each of claims 10 and 22. Further, Applicants respectfully submit that Tatebayashi fails to overcome the deficiencies of Pinder described above.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Applicants do not concede that the representations made more specifically by the Examiner with respect to dependent claims 10 and 22 are correct. However, Applicants submit that those other points are moot in view of the fact that the cited combination fails to teach or suggest the invention as recited in independent claims 1 and 13.

5. Comments on the Allowable Subject Matter

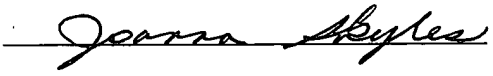
The Examiner stated that claims 11, 12, 23, 24, 29, and 35, objected to as being dependent upon a rejected base claim, would be allowable if rewritten in independent from including all of the limitations of the base claim and any intervening claims. As explained above, Applicants submit that base claims 1, 13, 25, and 31 are patentably distinguishable over Pinder. Consequently, Applicants submit that claims 11, 12, 23, 24, 29, and 35 are in condition for allowance as is, and that no amendment should be required.

6. Conclusion

Accordingly, Applicants respectfully submit that all of presently pending claims 1-4, 8-16, and 20-42 are in condition for allowance, and Applicants respectfully request favorable reconsideration.

Respectfully submitted,

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP

Date: November 9, 2004 By: 

Joanna Skyles
Reg. No. 54,454

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001